CLAIMS

What is claimed is:

1. An improved security processing circuit for performing 3DES IPsec security processing services for a host system using a DES engine, the security processing circuit comprising:

the DES engine having a message input, a cipher key input, and a pre-data output, the engine adapted to receive and selectively process a block of data from the message input of the security processing circuit during a first DES processing operation, and subsequently to process data from an intermediate result during second and third DES processing operations and store an intermediate result of the third DES processing operation to the pre-data output;

a security keys circuit having a set of cipher keys input and a key output, the security keys circuit operable to select and transfer a different cipher key to the key output coupled to the cipher key input of the DES engine selected from the set of cipher keys associated with each DES processing operation during the first, second and third DES processing operations; and

a data output circuit having a pre-data input and a data output, the pre-data input of the data output circuit coupled to the pre-data output of the DES engine, and the data output selectively coupleable to the host system, the data output circuit operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system.

2. The security processing circuit of claim 1, wherein the DES engine comprises:

a permutation block PB having the message input and a permutation output, the permutation block PB operable to receive a block of data at the message input and to perform an initial permutation of the message input data and provide a permutation result at the permutation output;

a data input multiplexor DI Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output;

an intermediate result register R_REG/L_REG having a data input, a clock input, and a latched data output, the register operable to store right and left half results of the initial permutation or of a cipher process based on data present at the data input upon receipt of a clock signal at the clock input;

eight cipher blocks having a data input, a key input, and a cipher output, operable to receive data at the data input and a key at the key input, to perform the cipher process comprising right and left halves of a sequential eight step cipher process on the data at the data input employing the key, and to provide a first and second cipher result during a first and second eight step cycle of each of the three DES processing operations;

a pre-data output multiplexor PDO Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output; and

a pre-data output register PRE_DO having a data input, a clock input, and a latched data output,

wherein the permutation output of the permutation block PB is coupled to the first input of the data input multiplexor DI Mux, the data selection output of the data input multiplexor DI Mux coupled to the data input of the intermediate result register R_REG/L_REG, the latched data output of the intermediate result register R_REG/L_REG coupled to the data input of the eight cipher blocks having the cipher output of the eight cipher blocks feedback coupled to the second input of the data input multiplexor DI Mux and to the first input of the pre-data output multiplexor PDO Mux 81e, the data selection output of the pre-data output multiplexor PDO Mux coupled to the pre-data output register PRE_DO, the latched data output of the pre-data output register PRE_DO feedback coupled to the second input of the pre-data output multiplexor PDO Mux and the pre-data output.

3. The security processing circuit of claim 2,

wherein the DES engine is further operable to perform the initial permutation of the message input data using the permutation block PB, initially select the permutation result with the data input multiplexor DI Mux and couple and store the result to the intermediate result register R_REG/L_REG during a data input latch cycle, to transfer the initial result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the first eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG during the first cipher process cycle, to transfer the stored intermediate result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the second eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG and the pre-data output register PRE_DO subsequent to selection of the first input of the pre-data output multiplexor PDO Mux during the second cipher process cycle of the first DES processing operation, and

wherein the DES engine is operable to repeat the first and second cipher process cycles for the subsequent second and third DES security processing operations of the security processing circuit, and latch the intermediate result of the third DES operation to the pre-data output of the pre-data output register PRE_DO of the DES engine, using the selection of the second input of the pre-data output multiplexor PDO Mux during the third DES processing operation of the 3DES security processing.

4. The security processing circuit of claim 3, wherein the 3DES processing is completed in three single DES processing operations.

5. The security processing circuit of claim 3, wherein the 3DES processing is completed in eight clock cycles.

6. The security processing circuit of claim 3, wherein the first, second and third DES processing operations each have a duration of two clock cycles.

7. The security processing circuit of claim 5, wherein the clock cycle has a period of about 8ns.

8. The security processing circuit of claim 5, wherein the eight clock cycles of the 3DES security processing comprise:

a data input latch cycle;

a first DES processing operation comprising two cycles;

a second DES processing operation comprising two cycles;

a third DES processing operation comprising two cycles; and

a data output latch cycle.

9. The security processing circuit of claim 1, further comprising a clock input coupled to one or more of the DES engine, the security keys circuit, and the data output circuit for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit.

10. The security processing circuit of claim 1, wherein the security keys circuit comprises:

a set of cipher keys input, wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing;

a keys input multiplexor Key Mux having a set of cipher keys input, and a cipher key selection output, the mux operable to select and couple a cipher key to the cipher key selection output; and

a security keys register SK_REG having a data input, a clock input, and a latched data output, the register operable to store the cipher key selection associated with one of the three DES processing operations of the 3DES security processing based on cipher key

data at the data input upon receipt of a clock signal at the clock input, the latched data output of the security keys register SK_REG coupled to the key input of the eight cipher blocks.

11. The security processing circuit of claim 10, wherein the keys input multiplexor Key Mux is operable to receive the three cipher keys and to selectively couple one of the three cipher keys associated with a DES processing operation to the DES engine during the three DES processing operations of the 3DES security process.

12. The security processing circuit of claim 1, wherein the data output circuit comprises:

an inverse permutation block IPB having a pre-data input and an inverse permutation output, the block operable to receive and further security process the pre-data output from the DES engine, performing an inverse permutation of the pre-data and transfer the processed data to the inverse permutation output;

an XOR gate XOR having a processed data input, an initialization vector input, and an XOR gate output, the XOR gate operable to selectively exclusive OR the initialization vector at the initialization vector input together with the processed data from the inverse permutation output of the inverse permutation block coupled to the processed data input, and transfer the XOR data to the XOR gate output;

a data output multiplexor DO Mux having a first and second input, a selection control signal, and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output, based on the state of the selection control signal, the first input coupled to the XOR gate output, and the second input coupled to a data output register DO_REG; and

the data output register DO_REG having a data input, a clock input, and a latched data output, the register operable to store the output data results of the third DES process based on data present at the data input upon receipt of a clock signal at the clock input, the latched data output of the data output register DO_REG feedback coupled to the

second input of the data output multiplexor DO Mux to insure latching of the data at the output,

wherein the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system.

13. The security processing circuit of claim 12, wherein the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system.

14. The security processing circuit of claim 1, wherein the security processing circuit resides within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a DES engine.

15. The security processing circuit of claim 1, further comprising a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively encrypt outgoing data from the host system to cryptographically process data for transmission to the network.

16. The security processing circuit of claim 15, wherein the network interface device comprises a bus interface, a media access control system, and the security processing circuit.

17. The security processing circuit of claim 16, wherein the network interface device is a single integrated circuit.

18. The security processing circuit of claim 1, wherein the circuit comprises an IPsec circuit adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data.

19. An improved DES engine used in a security processing circuit for performing 3DES IPsec security processing, the DES engine comprising:

a permutation block PB having the message input and a permutation output, the permutation block PB operable to receive a block of data at the message input and to perform an initial permutation of the message input data and provide a permutation result at the permutation output;

a data input multiplexor DI Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output;

an intermediate result register R_REG/L_REG having a data input, a clock input, and a latched data output, the register operable to store right and left half results of the initial permutation or of a cipher process based on data present at the data input upon receipt of a clock signal at the clock input;

eight cipher blocks having a data input, a key input, and a cipher output, operable to receive data at the data input and a key at the key input, to perform the cipher process comprising right and left halves of a sequential eight step cipher process on the data at the data input employing the key, and to provide a first and second cipher result during a first and second eight step cycle of each of the three DES processing operations;

a pre-data output multiplexor PDO Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output; and

a pre-data output register PRE_DO having a data input, a clock input, and a latched data output,

wherein the engine is adapted to receive and selectively process a block of data from the message input of the security processing circuit during a first DES processing operation, and subsequently to process data from an intermediate result during second and

third DES processing operations of a 3DES security processing and store an intermediate result of the third DES processing operation to a pre-data output of the pre-data output register PRE_DO, and

wherein the permutation output of the permutation block PB is coupled to the first input of the data input multiplexor DI Mux, the data selection output of the data input multiplexor DI Mux coupled to the data input of the intermediate result register R_REG/L_REG, the latched data output of the intermediate result register R_REG/L_REG coupled to the data input of the eight cipher blocks having the cipher output of the eight cipher blocks feedback coupled to the second input of the data input multiplexor DI Mux and to the first input of the pre-data output multiplexor PDO Mux, the data selection output of the pre-data output multiplexor PDO Mux coupled to the pre-data output register PRE_DO, the latched data output of the pre-data output register PRE_DO feedback coupled to the second input of the pre-data output multiplexor PDO Mux and the pre-data output.

20. The DES engine of claim 19,

wherein the engine is further operable to perform the initial permutation of the message input data using the permutation block PB, initially select the permutation result with the data input multiplexor DI Mux and couple and store the result to the intermediate result register R_REG/L_REG during a data input latch cycle, to transfer the initial result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the first eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG during the first cipher process cycle, to transfer the stored intermediate result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the second eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG and the pre-data output register PRE_DO subsequent to selection of the

first input of the pre-data output multiplexor PDO Mux during the second cipher process cycle of the first DES processing operation, and

wherein the DES engine is operable to repeat the first and second cipher process cycles for the subsequent second and third DES security processing operations of the security processing circuit, and latch the intermediate result of the third DES operation to the pre-data output of the pre-data output register PRE_DO of the DES engine, using the selection of the second input of the pre-data output multiplexor PDO Mux during the third DES processing operation of the 3DES security processing.

21. The DES engine of claim 19, wherein the timing of the 3DES processing is completed in three single DES processing operations.

22. The DES engine of claim 19, wherein the timing of the 3DES processing is completed in eight clock cycles.

23. The DES engine of claim 19, wherein the first, second and third DES processing operations each have a duration of two clock cycles.

24. The DES engine of claim 22, wherein the clock cycle has a period of about 8ns.

25. The DES engine of claim 22, wherein the eight clock cycles of the 3DES security processing comprise:

a data input latch cycle;

a first DES processing operation comprising two cycles;

a second DES processing operation comprising two cycles;

a third DES processing operation comprising two cycles; and

a data output latch cycle.

26. The DES engine of claim 19, further comprising a clock input coupled to one or more of the DES engine, the security keys circuit, and the data output circuit for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit.

27. A method of performing 3DES IPsec security processing in a security processing circuit utilizing a DES engine, after the circuit has performed an initial permutation of a data message input to the circuit, the method comprising:

selecting a permutation result of the initial permutation to couple the result to an intermediate result register during a first DES process;

storing the permutation result in the intermediate result register;

cipher processing the stored permutation result using an eight cipher blocks to generate an intermediate result of the cipher processing;

selectively storing the intermediate result in the intermediate result register;

cipher processing the stored intermediate result using the eight cipher blocks to generate a first DES result of the cipher processing; and

selectively storing the first DES result in the intermediate result register.

28. The method of claim 27, wherein a second DES process further comprises:

cipher processing the stored first DES result using the eight cipher blocks to generate a second intermediate result of the cipher processing;

selectively storing the second intermediate result in the intermediate result register;

cipher processing the stored second intermediate result using the eight cipher blocks to generate a second DES result of the cipher processing; and

selectively storing the second DES result in the intermediate result register.

29. The method of claim 28, wherein a third DES process further comprises:

cipher processing the stored second DES result using the eight cipher blocks to generate a third intermediate result of the cipher processing;

selectively storing the third intermediate result in the intermediate result register;

cipher processing the stored third intermediate result using the eight cipher blocks to generate a third pre-data DES result of the cipher processing;

selectively storing the third pre-data DES result in the intermediate result register and selectively storing the third pre-data DES result in a pre-data output register;

performing an inverse permutation of the third pre-data DES result;

exclusively ORing the result of the inverse permutation with an initialization vector to generate a 3DES result; and

selectively latching the 3DES result to a data output register.

30. A method of performing a single DES processing within a 3DES security processing circuit utilizing a DES engine, after the 3DES circuit has performed an initial permutation of a data message input to the circuit, the method comprising:

receiving data of a permutation result of the initial permutation to a data input multiplexor during a first DES process;

selecting and coupling the permutation result at the data input multiplexor to an intermediate result register;

storing the permutation result in the intermediate result register;

transferring the stored permutation result and a cipher key to an eight cipher blocks for cipher processing;

cipher processing using the eight cipher blocks to generate data of an intermediate result of the cipher processing;

storing the intermediate result in the intermediate result register;

transferring the stored intermediate result and the cipher key to the eight cipher blocks for cipher processing;

cipher processing the intermediate result data using the eight cipher blocks to generate a first DES result of the cipher processing; and

storing the first DES result in the intermediate result register.

31. The method of claim 30, wherein a second DES process further comprises:

cipher processing the stored first DES result using the eight cipher blocks to generate a second intermediate result of the cipher processing;

selectively storing the second intermediate result in the intermediate result register;

cipher processing the stored second intermediate result using the eight cipher blocks to generate a second DES result of the cipher processing; and

selectively storing the second DES result in the intermediate result register.

32. The method of claim 31, wherein a third DES process further comprises:

cipher processing the stored second DES result using the eight cipher blocks to generate a third intermediate result of the cipher processing;

selectively storing the third intermediate result in the intermediate result register;

cipher processing the stored third intermediate result using the eight cipher blocks to generate a third pre-data DES result of the cipher processing;

selectively storing the third pre-data DES result in the intermediate result register and selectively storing the third pre-data DES result in a pre-data output register;

performing an inverse permutation of the third pre-data DES result;

exclusively ORing the result of the inverse permutation with an initialization vector to generate a 3DES result; and

selectively latching the 3DES result to a data output register.

33. A method of performing a single DES processing within a 3DES security processing operation utilizing a DES engine, the method comprising:

selecting an input data block to an input data node of the DES engine using a data select switch during a first DES processing operation;

selecting a first key from the key data to a key data node of the DES engine using a key select switch during the first DES processing operation, the first key associated with the input data;

first DES processing the input data with the associated first key using the DES engine of the security processing circuit;

obtaining a first intermediate result data from the first DES processing operation at a DataOut bus of the security processing circuit, the intermediate result being feedback coupled to a feedback input of the data select switch;

selecting the intermediate result data to the input data node of the DES engine using the data select switch during a second DES processing operation; and

latching the intermediate result data into an intermediate result register.

34. A method of performing a DES processing within a 3DES security processing operation utilizing a DES engine of the security processing circuit, the method comprising:

coupling and storing data of a first intermediate result to an intermediate result register;

transferring the first intermediate result data from the register to a set of eight cipher blocks for cipher processing during a first cycle of the DES processing;

DES processing the data with an associated cipher key using the set of eight cipher blocks to produce a second intermediate result fed back to the intermediate result register;

storing the second intermediate result back into the intermediate result register;

transferring the second intermediate result data from the register to the set of eight cipher blocks for cipher processing during a second cycle of the DES processing;

DES processing the second intermediate result data with the associated cipher key using the set of eight cipher blocks to produce a third intermediate result fed back to the intermediate result register; and

storing the third intermediate result back in the intermediate result register on the second cycle of the DES processing.